UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,161	03/09/2004	John Fred Davis	END920030160US1	3025

26502 7590 11/27/2007

IBM CORPORATION
IPLAW SHCB/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
KESSLER, MATTHEW E	
ART UNIT	PAPER NUMBER
4121	

MAIL DATE	DELIVERY MODE
11/27/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/796,161	DAVIS ET AL.	
	Examiner	Art Unit	
	Matthew E. Kessler	4121	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/9/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.

2. Claims 1-20 are rejected.

Specification

3. The use of the trademark "Spam Assasin" has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology. The appropriate capitalization of the aforementioned trademark should be corrected.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

4. The disclosure is objected to because of the following informalities: The "Background of the Invention" section contains a missing citation of a trademark. Currently the disclosure reads as "(trademark of ___)". A correct citation of the trademark should be included.

Claim Rejections - 35 USC § 101

5. Claims 9-16 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 9-16 are directed to a "computer program product" and although claim 9 is limited to a computer readable medium, in the broadest reasonable

interpretation, computer readable medium is directed to non-statutory subject matter, i.e. a carrier wave. The specification does not limit the medium to a tangible storage medium.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1-4, 7, 9-12, 14, and 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Kirsch US Patent Application 2005/0198159 (hereinafter Kirsch).

As to claim 1, Kirsch teaches a method of blocking unwanted e-mails, said method comprising the steps of (The abstract teaches "An e-mail filtering method and system that categorizes received e-mail messages based on information about the origin…" Once an email is determined to be unwanted through filtering it is put on the "blacklist" and deleted or handled according to the user's preference. It is understood that deleting blacklisted emails is a form of blocking them.):

identifying an e-mail as unwanted (Paragraph [0086] teaches in "Referring again to FIG. 2, if the categorized e-mail does not seem to be spam (block 114), the message is sent to the recipient (for instance, the message is sent to the recipient's inbox) (block 104). However, if the

e-mail appears to be spam (block 114), it is sent to a spam folder (block 116)." In block 114 of Fig. 2, a determination is made if the received email is unwanted or not.);

determining a source IP address of the unwanted e-mail (Paragraph [0026] teaches "In this embodiment, if the sender or site is not on the blacklist (block 106), the actual sender of the message is determined (block 110). (In other embodiments, other information identifying the origin (sender and/or the site), such as final IP address, final domain name, normalized reverse DNS of the final IP address, IP path, etc. may be used.)" The IP is parsed from the email header to determine all sorts of information in use to identify the sender, including its final IP. This final IP is interpreted to be the source IP.);

determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail (Paragraph [0053] teaches "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." Here it is understood that the sender is identified by all sorts of means, one of which is disclosed is a netblock. The netblock is a series of IP addresses that would be owned by the same owner or registrant.); and

subsequently blocking e-mails from said source IP address and said other IP addresses (Paragraph [0054] teaches "Referring again to FIG. 2, once the actual sender is determined (block 110), the e-mail message is categorized based on other information about the actual

sender (block 112). (In other embodiments, a message can be categorized based on other information about the origin of the message, including the site, based on identifying information such as final IP address, final domain name (or nrDNS of the final IP address) or IP path based on the same approach described below). The information about the actual sender, as well as the recipient's determination of whether the message was solicited..." It is understood that the database which stores this information which previously described in paragraph [0053] listed netblocks. By blocking the sender including the netblock, DNS information, and other information, all IPs would be blocked.).

As to claim 2, Kirsch teaches the method as set forth in claim 1(Kirsch teaches all the limitations of claim 1.).

wherein the step of determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail comprises the step of determining an owner or registrant of said source IP address of said unwanted e-mail (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." It is understood that in one of Kirsch's embodiments, one way the original sender may be identified is through finding out the owner of the IP.).

As to claim 3, Kirsch teaches the method as set forth in claim 2 (Kirsch teaches all of the limitations of claim 2.)

wherein the step of determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail is performed by querying an entity that manages registration of IP addresses (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." Kirsch teaches the use of looking up owner data through the ARIN.).

As to claim 4, Kirsch teaches the method as set forth in claim 3 (Kirsch teaches all of the limitations of claim 3.)

wherein said entity is Internet Assigned Number Authority (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to

identify the sender or site regardless of whether nrDNS is available." The American Registry of Internet Numbers is a Regional Internet Registry (RIR) that is allocated Ipv4 addresses from the IANA services. It is interpreted that the lookup of owner data in the ARIN is looking up IANA owner information.).

As to claim 7, Kirsch teaches the method as set forth in claim 1 (Kirsch teaches all of the limitations of claim 1.)

wherein the step of determining a source IP address of the unwanted e-mail comprises the step of reading the source IP address from a header of the unwanted (Paragraph [0023] teaches that "the e-mail address may be combined with at least one other piece of information from the message header or SMTP session. This information includes fields such as the display name, the final IP address, x-mailer, final domain name, user-agent, information about the client software used by the sender, time zone, source IP address, the sendmail version used by a first receiver, and the MAIL FROM address." Both the source IP and final IP are listed as information which can be used from the email header.).

As to claim 9, Kirsch teaches a computer program product for blocking unwanted e-mails, said computer program product comprising (Paragraph [0021] teaches an embodiment of the invention as being a computer program which is stored on computer readable medium.):

a computer readable medium (Paragraph [0021] teaches the embodiment of a computer program which is stored and executed from a computer readable medium.);

first program instructions to identify an e-mail as unwanted (Paragraph [0086] teaches in "Referring again to FIG. 2, if the categorized e-mail does not seem to be spam (block 114), the message is sent to the recipient (for instance, the message is sent to the recipient's inbox) (block 104). However, if the e-mail appears to be spam (block 114), it is sent to a spam folder (block 116)." In block 114 of Fig. 2, a determination is made if the received email is unwanted or not.);

second program instructions to determine a source IP address of the unwanted e-mail (Paragraph [0026] teaches "In this embodiment, if the sender or site is not on the blacklist (block 106), the actual sender of the message is determined (block 110). (In other embodiments, other information identifying the origin (sender and/or the site), such as final IP address, final domain name, normalized reverse DNS of the final IP address, IP path, etc. may be used.)" The IP is parsed from the email header to determine all sorts of information in use to identify the sender, including its final IP. This final IP is interpreted to be the source IP.);

third program instructions to determine other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail (Paragraph [0053] teaches "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." Here it is understood that the sender is identified by all sorts of means, one of which is disclosed is a

netblock. The netblock is a series of IP addresses that would be owned by the same owner or registrant.);

and fourth program instructions to subsequently block e-mails from said source IP address and said other IP addresses (Paragraph [0054] teaches "Referring again to FIG. 2, once the actual sender is determined (block 110), the e-mail message is categorized based on other information about the actual sender (block 112). (In other embodiments, a message can be categorized based on other information about the origin of the message, including the site, based on identifying information such as final IP address, final domain name (or nrDNS of the final IP address) or IP path based on the same approach described below). The information about the actual sender, as well as the recipient's determination of whether the message was solicited..." It is understood that the database that stores this information that was previously described in paragraph [0053] listed netblocks. By blocking the sender including the netblock, DNS information, and other information, all IPs would be blocked.); and wherein

said first, second, third and fourth program instructions are recorded on said medium (Paragraph [0021] teaches the embodiment of a computer program which is stored and executed from a computer readable medium.).

As to claim 10, Kirsch teaches a computer program product as set forth in claim 9 (Kirsch teaches all of the limitations of claim 9.)

wherein said third program instructions determine an owner or registrant of said source IP address of said unwanted e-mail (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may

be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." It is understood that in one of Kirsch's embodiments, one way the original sender may be identified is through finding out the owner of the IP.).

As to claim 11, Kirsch teaches a computer program product as set forth in claim 10 (Kirsch teaches all of the limitations of claim 10.)

wherein said third program instructions determine an owner or registrant of said source IP address by querying an entity that manages registration of IP addresses (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." Kirsch teaches the use of looking up owner data through the ARIN.).

As to claim 12, Kirsch teaches a computer program product as set forth in claim 11 (Kirsch teaches all of the limitations of claim 11.)

wherein said entity is Internet Assigned Number Authority (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." The American Registry of Internet Numbers is a Regional Internet Registry (RIR) that is allocated Ipv4 addresses from the IANA services. It is interpreted that the lookup of owner data in the ARIN is looking up IANA owner information.).

As to claim 15, Kirsch teaches a computer program product as set forth in claim 9 (Kirsch teaches all of the limitations of claim 9.)

wherein said second program instructions determines a source IP address of the unwanted e-mail comprises by reading the source IP address from a header of the unwanted (Paragraph [0023] teaches that "the e-mail address may be combined with at least one other piece of information from the message header or SMTP session. This information includes fields such as the display name, the final IP address, x-mailer, final domain name, user-agent, information about the client software used by the sender, time zone, source IP address, the sendmail version used by a first receiver, and the MAIL FROM address." Both the source IP and final IP are listed as information which can be used from the email header.).

As to claim 17, Kirsch teaches a system for blocking unwanted e-mails, said system comprising (The abstract teaches "An e-mail filtering method and system that categorizes received e-mail messages based on information about the origin…" Once an email is determined to be unwanted through filtering it is put on the "blacklist" and deleted or handled according to the user's preference. It is understood that deleting blacklisted emails is a form of blocking them. Paragraphs [0021] and [0022] give and example of the kind of system the method and software would be operated on. A system is taught including databases, a network, personal computers as well as all of the disclosed means for the functionality of the method.):

means for identifying an e-mail as unwanted (Paragraph [0086] teaches in "Referring again to FIG. 2, if the categorized e-mail does not seem to be spam (block 114), the message is sent to the recipient (for instance, the message is sent to the recipient's inbox) (block 104). However, if the e-mail appears to be spam (block 114), it is sent to a spam folder (block 116)." In block 114 of Fig. 2, a determination is made if the received email is unwanted or not.);

means for determining a source IP address of the unwanted e-mail (Paragraph [0026] teaches "In this embodiment, if the sender or site is not on the blacklist (block 106), the actual sender of the message is determined (block 110). (In other embodiments, other information identifying the origin (sender and/or the site), such as final IP address, final domain name, normalized reverse DNS of the final IP address, IP path, etc. may be used.)" The IP is parsed from the email header to determine all sorts of information in use to identify the sender, including its final IP. This final IP is interpreted to be the source IP.);

means for determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail (Paragraph [0053] teaches "Other

information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." Here it is understood that the sender is identified by all sorts of means, one of which is disclosed is a netblock. The netblock is a series of IP addresses that would be owned by the same owner or registrant.); and

means for subsequently blocking e-mails from said source IP address and said other IP addresses (Paragraph [0054] teaches "Referring again to FIG. 2, once the actual sender is determined (block 110), the e-mail message is categorized based on other information about the actual sender (block 112). (In other embodiments, a message can be categorized based on other information about the origin of the message, including the site, based on identifying information such as final IP address, final domain name (or nrDNS of the final IP address) or IP path based on the same approach described below). The information about the actual sender, as well as the recipient's determination of whether the message was solicited…" It is understood that the database which stores this information that previously described in paragraph [0053] listed netblocks. By blocking the sender including the netblock, DNS information, and other information, all IPs would be blocked.).

As to claim 18, Kirsch teaches a system as set forth in claim 17 (Kirsch teaches all of the limitations of claim 17, and in paragraph [0021] and [0022] Kirsch teaches the system which is the means for the method of blocking emails.)

wherein said means for determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail comprises means for determining an owner or registrant of said source IP address of said unwanted e-mail (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." It is understood that in one of Kirsch's embodiments, one way the original sender may be identified is through finding out the owner of the IP.).

As to claim 19, Kirsch teaches a system as set forth in claim 18 (Kirsch teaches all of the limitations of claim 18, and in paragraph [0021] and [0022] Kirsch teaches the system which is the means for the method of blocking emails.)

wherein said means for determining other source IP addresses owned or registered by an owner or registrant of the source IP address of said unwanted e-mail comprises means for querying an entity that manages registration of IP addresses (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The

nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." Kirsch teaches the use of looking up owner data through the ARIN.).

As to claim 20, Kirsch teaches a system as set forth in claim 19 (Kirsch teaches all of the limitations of claim 19, and in paragraph [0021] and [0022] Kirsch teaches the system which is the means for the method of blocking emails.)

wherein said entity is Internet Assigned Number Authority (Paragraph [0053] teaches that "Other information identifying the origin of the message may be used in other embodiments. The nrDNS name may be used, if it exists, to identify the site (or the sender); if nrDNS is not available, the final IP address, a netblock (a range of consecutive IP addresses), or owner data stored in databases such as the American Registry of Internet Numbers (" ARIN") may be used instead. In other embodiments, the final IP address, netblock, or owner data may be used to identify the sender or site regardless of whether nrDNS is available." The American Registry of Internet Numbers is a Regional Internet Registry (RIR) that is allocated Ipv4 addresses from the IANA services. It is interpreted that the lookup of owner data in the ARIN is looking up IANA owner information.).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 5-6 and 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kirsch, (hereinafter Kirsch) United States Patent Application number 2005/0198156 in further view of Anselm Lambert's dissertation "Analysis of Spam" (hereinafter Lambert).

As to claim 5, Kirsch teaches the method as set forth in claim 1 (Kirsch teaches all of the limitations of claim 1) but does not teach wherein the step of identifying an e-mail as unwanted comprises the step of identifying an e-mail which is attempted to be sent to multiple recipients where the e-mail contains the same or substantially the same text.

However in an analogous art, Lambert teaches wherein the step of identifying an e-mail as unwanted comprises the step of identifying an e-mail which is attempted to be sent to multiple recipients where the e-mail contains the same or substantially the same text (On page 74 of Lambert's dissertation he is addressing the issue when spammers change the subject of their emails to avoid filters. He mentions very clearly "E-mail administrators and some filters might view an e-mail message with the same subject going to multiple recipients as a spam message." It is understood that it was well known in the art that email messages that had the same subject being sent to multiple recipients is a determination of a message as spam. It is interpreted that if a message has the same subject line then it contains the same or substantially the same text.).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Kirsch's method for handling spam with Lambert's method for identifying spam. In paragraph [0006] of Kirsch's patent application, it is suggested that there already exist current techniques for identifying spam, one such method disclosed is through the use of hash functions. Lambert more clearly describes that an email sent to multiple recipients with the same subject can be identified as spam. It would be obvious once spam was identified using Lambert's teaching to block it according to the teachings of Kirsch.

As to claim 6, Kirsch teaches the method as set forth in claim 1 (Kirsch teaches all of the limitations of claim 1) but does not teach wherein the step of identifying an e-mail as unwanted comprises the step of identifying an e-mail which is attempted to be sent to multiple recipients where the e-mail contains the same or substantially the same subject line.

However in an analogous art, Lambert teaches wherein the step of identifying an e-mail as unwanted comprises the step of identifying an e-mail which is attempted to be sent to multiple recipients where the e-mail contains the same or substantially the same subject line (Page 74 of Lambert's dissertation teaches "E-mail administrators and some filters might view an e-mail message with the same subject going to multiple recipients as a spam message." It is understood that it was well known in the art that email messages that had the same subject being sent to multiple recipients is a determination of a message as spam.).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Kirsch's method for handling spam with Lambert's method for identifying spam. In paragraph [0006] of Kirsch's patent application, it is suggested that there already exist current techniques for identifying spam, one such method disclosed is through the use of hash functions. Lambert more clearly describes that an email sent to multiple recipients with the same subject can be identified as spam. It would be obvious once spam was identified using Lamberts teaching to block it according to the teachings of Kirsch.

As to claim 13, Kirsch teaches a computer program product as set forth in claim 9 (Kirsch teaches all of the limitations of claim 9) but does not teach wherein said first program

instructions identifies an e-mail as unwanted by identifying an e-mail which is attempted to be sent to multiple recipients where the e-mail contains the same or substantially the same text.

However in an analogous art, Lambert teaches wherein said first program instructions identifies an e-mail as unwanted by identifying an e-mail which is attempted to be sent to multiple recipients where the e-mail contains the same or substantially the same text (On page 74 of Lambert's dissertation he is addressing the issue when spammers change the subject of their emails to avoid filters. He mentions very clearly "E-mail administrators and some filters might view an e-mail message with the same subject going to multiple recipients as a spam message." It is understood that it was well known in the art that email messages that had the same subject being sent to multiple recipients is a determination of a message as spam. It is interpreted that if a message has the same subject line then it contains the same or substantially the same text.).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Kirsch's program for handling spam with Lambert's method for identifying spam. In paragraph [0006] of Kirsch's patent application, it is suggested that there already exist current techniques for identifying spam, one such method disclosed is through the use of hash functions. Lambert more clearly describes that an email sent to multiple recipients with the same subject can be identified as spam. It would be obvious once spam was identified using Lambert's teaching to block it according to the teachings of Kirsch.

As to claim 14, Kirsch teaches A computer program product as set forth in claim 9 (Kirsch teaches all of the limitations of claim 9) but does not teach wherein said first program instructions identifies an e-mail as unwanted by identifying an e-mail which is attempted to be

sent to multiple recipients where the e-mail contains the same or substantially the same subject line.

However in an analogous art, Lambert teaches wherein said first program instructions identifies an e-mail as unwanted by identifying an e-mail which is attempted to be sent to multiple recipients where the e-mail contains the same or substantially the same subject line. (Page 74 of Lambert's dissertation teaches "E-mail administrators and some filters might view an e-mail message with the same subject going to multiple recipients as a spam message." It is understood that it was well known in the art that email messages that had the same subject being sent to multiple recipients is a determination of a message as spam.).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Kirsch's program for handling spam with Lambert's method for identifying spam. In paragraph [0006] of Kirsch's patent application, it is suggested that there already exist current techniques for identifying spam, one such method disclosed is through the use of hash functions. Lambert more clearly describes that an email sent to multiple recipients with the same subject can be identified as spam. It would be obvious once spam was identified using Lamberts teaching to block it according to the teachings of Kirsch.

8. Claims 8 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kirsch, (hereinafter Kirsch) United States Patent Application number 2005/0198156 in further view of Barracuda Network's product publication "Barracuda Spam Firewall" (hereinafter Barracuda).

As to claim 8, Kirsch teaches the method as set forth in claim 1 (Kirsch teaches all of the limitations of claim 1) but does not teach wherein the step of subsequently blocking e-mails from said source IP address and said other IP addresses comprises the step of identifying said e-mails from said source IP address and said other IP addresses at a firewall or router, and then preventing them from passing through to a mail server(s) for their intended recipients.

However in an analogous art, Barracuda teaches wherein the step of subsequently blocking e-mails from said source IP address and said other IP addresses comprises the step of identifying said e-mails from said source IP address and said other IP addresses at a firewall or router, and then preventing them from passing through to a mail server(s) for their intended recipients (The sixth paragraph of Barracuda's product publication teaches "The Barracuda Spam Firewall provides powerful and scalable spam-blocking capabilities. It can handle over 10 million messages a day - filtering out both spam and viruses without bogging down your email servers. In fact, the Barracuda Spam Firewall actually reduces the load on your email servers because it operates independently.").

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Kirsch's methods of blocking spam with Barracuda Network's teaching of blocking spam on a firewall because as Barracuda's product publication suggests "the Barracuda Spam Firewall actually reduces the load on your email servers because it operates independently."

As to claim 16, Kirsch teaches a computer program product as set forth in claim 9 (Kirsch teaches all of the limitations of claim 9) but does not teach wherein said fourth program

instructions blocks e-mails from said source IP address and said other IP addresses by identifying said e-mails from said source IP address and said other IP addresses at a firewall or router, and then preventing them from passing through to a mail server(s) for their intended recipients.

However in an analogous art, Barracuda teaches wherein said fourth program instructions blocks e-mails from said source IP address and said other IP addresses by identifying said e-mails from said source IP address and said other IP addresses at a firewall or router, and then preventing them from passing through to a mail server(s) for their intended recipients. (The sixth paragraph of Barracuda's product publication teaches "The Barracuda Spam Firewall provides powerful and scalable spam-blocking capabilities. It can handle over 10 million messages a day - filtering out both spam and viruses without bogging down your email servers. In fact, the Barracuda Spam Firewall actually reduces the load on your email servers because it operates independently.").

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to combine Kirsch's program of blocking spam with Barracuda Network's teaching of blocking spam on a firewall because as Barracuda's product publication suggests "the Barracuda Spam Firewall actually reduces the load on your email servers because it operates independently."

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Barchi, Patent Number 6507866, directed to email pattern detection;

Kirsch, Patent Application Number 2004/0177120, directed to filtering email messages;

Kirsch Patent Number 6546416, directed to selectively blocking bulk email;

Lu, Patent Number 7174453, directed to a message screening system;

Malik et al., Patent Application Number 2007/0083606, directed to spam blocking;

Murray, Patent Application Number 2005/0080855, directed to an email whitelist;

Shannon et al., Patent Application Number 2005/0198160, directed to identifying email styles.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Kessler whose telephone number is (571) 270-5005. The examiner can normally be reached on Monday through Friday 7:30 am - 5:00 pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Taghi T. Arani/
Supervisory Patent Examiner, Art Unit 4121

11/20/2007